UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/824,823	04/14/2004	Keisuke Takemori	61230 (47762)	6683

7590 04/03/2008

Edwards & Angell, LLP
Intellectual Property Practice Group
P.O. Box 55874
Boston, MA 02205

EXAMINER	
OKORONKWO, CHINWENDU C	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
04/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/824,823	TAKEMORI ET AL.	
	Examiner	Art Unit	
	CHINWENDU C. OKORONKWO	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. In response to communications filed on 01/16/2008, applicant amends claims 1, 11 and 21. The following claims, claims 1-30 are presented for examination.

Response to Remarks/Arguments

2. Applicant's arguments, pages 11-13, with respect to the rejection of claims 1-30 have been fully considered but they are not persuasive.

2.2 In response to Applicant argument that the Douglas in view of Maier references do not teach or suggest support apparatus arrange separately from the intrusion detection system, the Examiner respectfully disagrees citing column 2 lines 29-58 which recites "detects attacks targeted at the host system on which it is installed, e.g. on a web server 1, a domain name server, a mail server etc." and "monitors logs of applications running on the host ... monitor system files via its file integrity checking feature ... notifying the IDS administrator when key system and security files have been accessed, modified or even deleted" which clearly distinguishes the separation between the servers and host systems.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Douglas et al. (US Patent No. 7,152,242 B2) and further in view of Maier et al. (US Patent No. 5,625,815).

Regarding claims 1, 11 and 21, Douglas, discloses an IDS log analysis support apparatus, method and program comprising: a log collection section that collects a log of an intrusion detection system that is connected to a telecommunication network (col. 2 lines 17-20 – "host-based [intrusion detection system IDS sensor (HIDS)that detects attacks targeted at the host system on which it is installed, e.g. on a web server, a domain name server, a mail server, etc."); and a log analysis section that obtains statistics of the logs managed by the database and analyses the statistics, where the support apparatus is arrange separately from the IDS (col. 2 lines 29-35 – "detects attacks by monitoring the output to the

system and audit logs").

> Douglas is silent in disclosing a database that stores and manages logs collected by the log collection section, however Maier et al. does disclose such a database. It would have been obvious at the time of the invention, for one of ordinary skill in the art to modify the host based intrusion detection system of Douglas to make use of a database as this is an efficient means of managing a large quantities of data, such as intrusion detection logs and would benefit the invention by providing state of the art data management.

Regarding claims 2, 12 and 22, Douglas, discloses the IDS log analysis support apparatus, method and program according to claim 1, wherein the log analysis section comprises an internal and external similarity analysis device that sequentially compares an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, with an outward log in the logs, which is a log of accesses made from the protected subject side to the non-protected subject side, and sequentially calculates a degree of similarity that shows an extent to which the inward log and the outward log match based on the result of the comparison, and determines whether or not an abnormality has occurred based on the degree of similarity (col. 2 lines 29-58 – "detects attacks

targeted at the host system on which it is installed, e.g. on a web server 1, a domain name server, a mail server etc." and "monitors logs of applications running on the host ... monitor system files via its file integrity checking feature ... notifying the IDS administrator when key system and security files have been accessed, modified or even deleted.").

Regarding claims 3, 13 and 23, Douglas, does not explicitly disclose the IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises an access country analysis device that, taking as a subject to be detected a name of a country to which belongs a transmission source of an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, allocates a ranking to occurrence frequencies of country names, and determines that an abnormality has occurred when there is a change in the ranking of the country names that are normally detected, however it would have been obvious, to one of ordinary skill in the art, at the time of the invention to modify the disclosed "IP Address" of Douglas to be translated / traced to the originating country. The benefit of such modification would be to extend the usefulness of data that is already being collected by the invention to provide more information of the source of an attack (Rejected under the same rationale as claims 2, 12, 22, column 13 lines 51-67 and column 14 lines 1-10).

Regarding claims 4, 14 and 24, Douglas, does not explicitly disclose the IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises an access country analysis device that, taking as a subject to be detected a name of a country to which belongs a transmission source of an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, determines that an abnormality has occurred when there is an increase in the occurrence frequency of a country name that is not normally detected, however it would have been obvious, to one of ordinary skill in the art, at the time of the invention to modify the disclosed "IP Address" of Douglas to be translated / traced to the originating country. The benefit of such modification would be to extend the usefulness of data that is already being collected by the invention to provide more information of the source of an attack (Rejected under the same rationale as claims 2, 12, 22, col. 13 lines 51-67 and col. 14 lines 1-10).

Regarding claims 5, 15 and 25, Douglas, does not explicitly disclose the IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises an access country analysis device that, taking as a subject to be detected a name of a country to which belongs a transmission destination of an outward log in the logs, which is a log of accesses made from a protected subject side of the intrusion detection system to a non-protected subject side of the

intrusion detection system, allocates a ranking to occurrence frequencies of country names, and determines that an abnormality has occurred when there is a change in the ranking of the country names that are normally detected, however it would have been obvious, to one of ordinary skill in the art, at the time of the invention to modify the disclosed "IP Address" of Douglas to be translated / traced to the originating country. The benefit of such modification would be to extend the usefulness of data that is already being collected by the invention to provide more information of the source of an attack (Rejected under the same rationale as claims 2, 12, 22, col. 13 lines 51-67 and col. 14 lines 1-10).

Regarding claims 6, 16 and 26, Douglas, discloses IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises an access country analysis device that, taking as a subject to be detected a name of a country to which belongs a transmission destination of an outward log, which is a log of accesses made from a protected subject side of the intrusion detection system to a non-protected subject side of the intrusion detection system that are in the logs, determines that an abnormality has occurred when there is an increase in the occurrence frequency of a country name that is not normally detected, however it would have been obvious, to one of ordinary skill in the art, at the time of the invention to modify the disclosed "IP Address" of Douglas to be translated / traced to the originating country. The benefit of such modification would be to extend the usefulness of data that is already being collected by the

invention to provide more information of the source of an attack (Rejected under the same rationale as claims 2, 12, 22, col. 13 lines 51-67 and col. 14 lines 1-10).

Regarding claims 7, 17 and 27, Douglas, discloses the IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises a ratio analysis device that compares a short term number of events, which is the number of a predetermined event contained in a predetermined unit time period in the logs, with an average value of a short term number of events for a plurality of the unit time periods, and determines whether or not an abnormality has occurred based on a ratio of the short term number of events relative to the average value (col. 4 lines 61-67 and col. 5 lines 1-8 – "when a configured time interval elapses, a new instance of the EDE module is then started providing the previous instance has terminated").

Regarding claims 8, 18 and 28, Douglas, Is silent in disclosing the IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises a threshold learning device that calculates a short term number of events, which is the number of a predetermined event contained in a predetermined unit time period in the logs, and an average value of a short term number of events for a plurality of the unit time periods, and a standard deviation value of a short term number of events for a plurality of the unit time periods, and determines whether or not an abnormality has occurred using a result obtained

by dividing a difference between the short term number of events of a subject being investigated and the average value by the standard deviation value, however it would have been obvious, to one of ordinary skill in the art, at the time of the invention to modify the disclosed module callback functionality in which modules are started and terminated according to event detections and execute for preset time periods (col. 4 lines 61-67 and col. 5 lines 1-8 – "when a configured time interval elapses, a new instance of the EDE module is then started providing the previous instance has terminated").

Regarding claims 9, 19 and 29, Douglas, discloses the IDS log analysis support apparatus according to claim 1, wherein a plurality of intrusion detection systems are connected to the telecommunication network, and the plurality of intrusion detection systems each have a different protected subject, and the log analysis section comprises an IDS comparison device that compares a monitored profile, which is characteristics of logs of a monitored intrusion detection system, which is one intrusion detection system from among the plurality of intrusion detection systems, with an integrated profile, which is characteristics of logs of all the intrusion detection systems other than the monitored intrusion detection system from among the plurality of intrusion detection systems, and determines that an abnormality has occurred when the difference between the monitored profile and the integrated profile is equal to or greater than a predetermined value (col. 4 lines 31-37 – "scheduled modules (modules that are expected to terminate and

start again at fixed intervals), the AE monitors the schedule and starts these modules at the proper time").

Regarding claims 10, 20 and 30, Douglas, discloses the IDS log analysis support apparatus according to claim 9, wherein the IDS comparison device comprises a variable state comparison device that compares a variable state that accompanies an elapsed time of the monitored profile with a variable state that accompanies an elapsed time of the integrated profile, and determines that an abnormality has occurred when the difference between the variable states is equal to or greater than a predetermined value (col. 4 lines 61-67 and col. 5 lines 1-8 – "when a configured time interval elapses, a new instance of the EDE module is then started providing the previous instance has terminated").

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 9:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./

Examiner, Art Unit 2136

April 3, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136